41

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	
Wataru INOHA et al.	
Serial No. 09/733,057	Art Unit: 2134
Filed: December 11, 2000	Examiner: Nalven, Andrew L.
For: CRYPTOSYSTEM-RELATED METHOD AND APPARATUS	Atty Docket: 0102/0150

RESPONSE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The following is in response to the Office Action dated July 1, 2004 in which claims 1-16 were rejected under 35 U.S.C. 103(a) as being obvious over Miyano (U.S. Patent Number 5,442,705) in view of Applied Cryptography by Schneier.

The features of the method set forth in claim 1 include the step (1) of executing logical operation among bits in each of the blocks and generating a bit being a result of the logical operation, and the step (2) of combining the logical-operation-result bits into a second bit sequence.

The Examiner refers to Miyano (U.S. Patent Number 5,442,705), column 3, lines 30-34, in alleging that Miyano discloses the step (1) of executing logical operation among bits in each of the blocks and generating a bit being a result of the logical operation.

Column 3, lines 30-34 of Miyano reads: "Bit data Cn and Dn (n=1, 2, . . . , 16) obtained through the left circular shifts, are then decreased in number from 56 bits to 48 bits via permutation PC-2 shown in Table 3."

According to Table 3 in Miyano, a 56-bit sequence composed of bits b1, b2, b3, b4, b5, b6, b7, b8, b9, b10, b11, b12, b13, b14, b15, b16, b17, b18, b19, b20, b21, b22, b23, b24, b25, b26, b27, b28, b29, b30, b31, b32, b33, b34, b35, b36, b37, b38, b39, b40, b41, b42, b43, b44, b45, b46, b47, b48, b49, b50, b51, b52, b53, b54, b55 and b56 is rearranged into a 48-bit sequence composed of bits b14, b17, b11, b24, b1, b5, b3, b28, b15, b6, b21, b10, b23, b19, b12, b4, b26, b8, b16, b7, b27, b20, b13, b2, b41, b52, b31, b37, b47, b55, b30, b40, b51, b45, b33, b48, b44, b49, b39, b56, b34, b53, b46, b42, b50, b36, b29 and b32 by transposition (changing the positions of bits).

Thus, the bits composing the 48-bit sequence are the same as 48 bits from among the 56 bits composing the 56-bit sequence. Accordingly, in Miyano, logical operation among the 56 bits composing the 56-bit sequence is not executed. In Miyano, the transposition, that is, the change of the positions of bits, is implemented by permutation. Generally, the logical operation among bits significantly differs from the change of the positions of bits.

Therefore, it is respectfully submitted that Miyano does not teach the step (1) of executing logical operation among bits in each of the blocks and generating a bit being a result of the logical operation in claim 1.

It is further respectfully submitted that since Miyano does not teach logical operation among bits (the step (1)), Miyano therefore does not and could not teach the step (2) of combining the logical-operation-result bits into a second bit sequence in claim 1 also.

Schneier does not teach the step (1) of executing logical operation among bits in each of the blocks and generating a bit being a result of the logical operation, and the step

(2) of combining the logical-operation-result bits into a second bit sequence as set forth in claim 1.

Accordingly, it is respectfully submitted that claim 1 is patentable over Miyano and Schneier.

The methods and apparatuses in claims 2-16 each have features that are similar to the above-indicated features of the method in claim 1. Accordingly, it is respectfully submitted that claims 2-16 each are also patentable over Miyano and Schneier.

The features of the present invention is further explained herein with reference to claim 1 and Fig. 3 in the present application.

In the present invention, a first bit sequence is composed of a plurality of bits, and the first bit sequence represents information being a base of a key. The bits composing the first bit sequence is rearranged in a first matrix (M1) according to a predetermined arrangement rule. A plurality of blocks is formed in the first matrix (MI). Each of the blocks has bits, the number of which being smaller than the number of bits composing the first matrix (MI). For example, bits a11, a12, a21, and a22 compose one block (see Fig. 3). Logical operation is executed among bits in each of the blocks to generate a bit, which is thereby the result of the logical operation. The logical-operation-result bits are combined into a second bit sequence. The number of bits composing the second bit sequence is smaller than the number of bits composing the first bit sequence. The above procedure is the "FIRST STEP" in Fig. 3.

The method in claim 1 and Fig. 3 is a combination of the above "FIRST STEP" and the "SECOND STEP" using an S-Box. The method in claim 9 and Fig. 6 includes the "FIRST STEP" and the "SECOND STEP" in Fig. 3 which are combined in a reversed order.

The Examiner alleges that each of stages of the above "FIRST STEP" is disclosed by Miyano, and Schneier discloses an S-Box used in the DES (Data Encryption Standard). Then, the Examiner alleges that claims 1-16 are unpatentable over Miyano and Schneier.

It is respectfully submitted that the Examiner has misunderstood the contents of Miyano.

In Miyano, as disclosed in column 2, lines 65-66, a 64-bit initial key including 8 parity bits is inputted into a key scheduling section 10. As disclosed in column 3, line 15, the parity bits are discarded. As explained in the "Description of the Related Art" in the specification of the present application, DES prescribes that 8 bits among 64 bits are assigned to parities, and hence a substantial encryption key is composed of 56 bits. Discarding the parity bits is completely different from executing logical operation among bits in each of the blocks and getting a second bit sequence whose bit number is smaller than that of the first bit sequence in the present invention.

In Miyano, the permutation PC-1 is implemented by referring to Table 1, and 8 bits (parity bits) among 64 bits are discarded to get 56 bits. The 56 bits are divided into two blocks C and D each having 28 bits. According to Table 2, the blocks C and D are successively circularly shifted left to derive each key Kn (see column 3, lines 19-23). According to Table 3, permutation PC-2 including a step of discarding 8 bits rearranges the 56 bits obtained through the left circular shifts into 48 bits. The 16 keys K1-K16 are respectively applied to the stages S1-S16 in Fig. 1, and calculation and encryption are carried out.

As understood from the above explanation, Miyano does not teach rearranging the bits composing the first bit sequence in a first matrix (M1) according to a predetermined arrangement rule, and forming a plurality of blocks in the first matrix (M1). Each of the blocks has bits, the number of which is smaller than the number of bits composing the first matrix (M1). Nor does Miyano teach executing logical operation among bits in each of the

blocks, and thereby generating a bit being a result of the logical operation. Further, Miyano does not teach combining the logical-operation-result bits into a second bit sequence. The number of bits composing the second bit sequence is smaller than the number of bits composing the first bit sequence. In Miyano, merely transposition and circular shift are carried out. The "FIRST STEP" in Fig. 3 of the present invention therefore clearly differs from the contents of Miyano. In this regard, claims 1-16 are distinguished from Miyano.

The present invention accordingly can not be obtained by combining Miyano and Schneier. Accordingly, the instant invention is patentably distinguishable over the combination of Miyano and Schneier.

In light of the foregoing, the examiner is respectfully requested to reconsider the application and pass the same to issue at an early date.

Respectfully submitted,

Louis Woo, RN 31,730
Law Offices of Louis Woo
717 North Fayette Street
Alexandria, VA 22314
(703) 299-4090

Date: Sept 15, 2004